REMARKS

Favorable reconsideration of the application is respectfully requested in light of the amendments and remarks herein.

Upon entry of this amendment, claims 1-5, 8-15, and 18-21 are pending. No new matter has been added.

§103 Rejection of Claims 1-5, 8-15, and 18-21

In Section 4 of the Office Action, claims 1-5, 8-15, and 18-21 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Misra *et al.* (U.S. Patent 5,757,920; hereinafter referred to as "Misra") in view of Haber *et al.* (U.S. Patent 5,781,629; hereinafter referred to as "Haber"). This rejection is respectfully traversed below.

In the Specification, it is stated:

> Generally there are the following four important aspects of secure communication setup between two communicating parties:
>
> - Assurance that the originating communication partner is authorised to establish the connection (source is authentic),
>
> - assurance that the receiving communication partner is authorised (destination is authentic),
>
> - assurance that the received message was sent by the originating communication partner, and
>
> - assurance that the sent and received message has not been altered.

Background of the Specification, page 1, line 25 to page 2, line 1.

It is further stated:

> [Therefore, t]he very first and initial communication step in communication setup (e.g. the login procedure) is susceptible to copy or replay attacks which send a copy of communication setup (e.g. a

> user name and password recorded from a login procedure) to the communication partner. This problem is usually solved with additional knowledge about the communication partner at the other side and/or using large random session keys or transaction keys (usually taken from a transaction hearing).
>
> *Background of the Specification, page 2, lines 19-24.*

Therefore, the Background highlights the need to provide for a technique for reducing the risk of copy or replay attacks particularly in the first step of a communication setup in a more efficient way.

To achieve the above-stated objective, embodiments of the present invention provide methods and systems to authenticate data communicated from an originator to a destination. For example, the method of authenticating data communicated from an originator to a destination, as recited in claim 1, includes:

> *wherein* a keyed hashing technique is used, according to which data to be authenticated is concatenated with a private key and then processed with a cryptographic hash function and the data are transmitted together with the digest of the hash function from the originator to the destination,
> characterized in that
>
> *the data* comprises temporal validity information representing the temporal validity of the data;
>
> *the originator* receives an acknowledgement key from the destination, wherein the acknowledgement key includes a time stamp; and
>
> *the originator* verifies the acknowledgment key on the basis of the time stamp and the previously stored temporal validity information.
>
> *(emphasis added)*

Accordingly, in one aspect of claim 1, the originator verifies the acknowledgment key on the basis of the time stamp and the previously stored temporal validity information.

This limitation is included in the Specification as follows:

> In phase 2 the receiver generates a TSCS acknowledgement key and sends it to the receiver. The acknowledgement key consists of a new random bit array (independent from the originator) and the unified system time of the receiver.
>
> In phase 3 the originator checks the acknowledgement key (i.e. the digest and temporal validity), takes the random bit field of the acknowledgement key and merges it with the message data which is intended to be sent. The data (consisting of the message and the random field) is signed and sent to the receiver.
>
> Then the receiver checks in phase 4 the message digest and the identity of random bit field (from the message) and the previously generated random bit array of the acknowledgement key. If the message digest is valid and the bit arrays are identical, the message has mot been altered AND was generated as a result of the previous exchange of login and acknowledgement keys. The receiver sends then an acknowledgement to the communication originator.

Specification, page 7, lines 4-18, emphasis added.

> PHASE 3:
>
> **Message transmission**
>
> a) verification of the acknowledgement key authenticity and validity
>
> b) check the acknowledgement key signature (the digest)
>
> c) calculate own HMAC using private key K
> d) compare own HMAC with acknowledgement key digest
>
> e) check the acknowledgement key temporal validity
>
> f) calculate the difference between acknowledgement key universal time and current time (of the originator).
> g) check if time difference (absolute value) is less then the temporal validity of the acknowledgement key

Specification, page 9, lines 10-21, emphasis added.

Thus, the Specification clearly indicates that the originator verifies the acknowledgment key on the basis of the time stamp and the previously stored temporal validity information, for example, by calculating the difference between acknowledgement key universal time and current time (of the originator) and checking if the time difference (absolute value) is less then the temporal validity of the acknowledgement key.

By contrast, although Misra discloses that "[t]he logon certificate 110 also contains information such as the time the logon certificate was issued, the time of expiration of the logon certificate and the time at which the logon certificate becomes valid (i.e., start time)" (*Misra, col. 5, lines 51-55*), Misra fails to teach or suggest having the originator verify the acknowledgment key on the basis of the time stamp (i.e., the original time stamp) and the previously stored temporal validity information (e.g., the acknowledgement key universal time). Further, although Haber states generally that "[w]hen any user is presented with a digital document and its time-stamp certificate, the user can validate that the given certificate was indeed computed for the given document at the time claimed; if that is not the case, then the (document, certificate) pair will fail the validation or authentication test" (*Haber, col. 1, line 66 to col. 2, line 4*), Haber also fails to teach or suggest having the originator verify the acknowledgment key on the basis of the time stamp (i.e., the original time stamp) and the previously stored temporal validity information (e.g., the acknowledgement key universal time). Therefore, Misra and Haber, individually or in combination, fail to teach or suggest all the limitations of claim 1.

Based on the foregoing discussion, claim 1 should be allowable over Misra and Haber. Independent claims 5, 11, and 15 closely parallel claim 1 and recite substantially similar limitations as recited in independent claim 1. Therefore claims 5, 11, and 15 should also be allowable over Misra and Haber. Since claims 2-4, 8-10, 12-14, and 18-21 depend from one of

claims 1, 5, 11, and 15, claims 2-4, 8-10, 12-14, and 18-21 should also be allowable over Misra and Haber.

Accordingly, it is submitted that the rejection of claims 1-5, 8-15, and 18-21 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

Newly Added Claims

Claims 22-25 have been newly added. Claims 22-24 depend from claim 1. Therefore, claims 22-24 should be allowable over the cited prior art references. Claim 25 recites a method of authenticating transmission of messages comprising:

> *generating* a login key using a keyed-hashing method based on first random data, temporal validity information and a private key;
> transmitting the login key from an originator to a destination side;
> verifying the authenticity and the temporal validity of the login key based on a keyed hashing digest on the destination side;
>
> *generating* an acknowledgment key using the keyed-hashing method based on second random data and the private key, wherein the acknowledgement key includes a time stamp when the verification of the authenticity and the temporal validity of the login key is positive;
>
> *transmitting* the acknowledgment key from the destination side to the originator;
>
> *verifying* the acknowledgment key by the originator including checking the acknowledgement key based on the time stamp and the previously stored temporal validity information whether the acknowledgment key is still valid; and
>
> *adjusting* the time stamp and the originator upon receipt of the authentication messages based on a universal time field included in the messages.

Therefore, claim 25 includes all the limitations of claim 5 and an additional limitation of adjusting the time stamp and the originator upon receipt of the authentication messages based on a universal time field included in the messages. Accordingly, based on the foregoing discussion regarding claim 5, claim 25 should also be allowable over the cited prior art references.

CONCLUSION

In view of the foregoing, entry of this amendment, and the allowance of this application with claims 1-5, 8-15, and 18-21 is respectfully solicited.

In regard to the claims amended herein and throughout the prosecution of this application, it is submitted that these claims, as originally presented, are patentably distinct over the prior art of record, and that these claims were in full compliance with the requirements of 35 U.S.C. §112. Changes to these claims, as presented herein, are not made for the purpose of patentability within the meaning of 35 U.S.C. §§101, 102, 103 or 112. Rather, these changes are made simply for clarification and to round out the scope of protection to which Applicants are entitled.

In the event that additional cooperation in this case may be helpful to complete its prosecution, the Examiner is cordially invited to contact Applicants' representative at the telephone number written below.

The Commissioner is hereby authorized to charge any insufficient fees or credit any overpayment associated with the above-identified application to Deposit Account 50-0320.

Respectfully submitted,

FROMMER LAWRENCE & HAUG LLP

By: Samuel S. Lee, Reg. No. 42,791 for
William S. Frommer
Reg. No. 25,506
(212) 588-0800